# Exhibit 2

*CONFIDENTIAL*

**Work Order for Red Teaming and Infrastructure Penetration Testing.**

1. **Parties to the Work Order and Contract.**

Vital Management Services,Inc (**Client**) and Cyber Defence and Analytics (**CyberDnA**) enter into this Work Order as a Contract for performing red teaming and infrastructure penetration testing. This Work Order describes Services CyberDnA will provide to Client.

2. **Confidentiality**

Services shall be performed in a manner that maintains Client's assertion of legal privilege regarding Client's communications, documentation and other information made available from its computer systems and networks. CyberDnA understands that Client considers communications between and among CyberDnA and Client in connection with this Work Order to be kept confidential. These protections are Client's and not CyberDnA's, and these privileges and protections may only be waived by Client its sole discretion.

Furthermore, all documents, including but not limited to notes, diagrams, charts, analyses, reports and summaries, in print or digital media, whether completed or in draft form, created by CyberDnA under this Work Order shall be deemed Client's "Confidential" work product prepared for the sole purpose of client only. CyberDnA will take reasonable, necessary and prudent steps to maintain the confidentiality of information related to this Work Order. Accordingly, CyberDnA will maintain as confidential all information and data it receives from Client, and will not disclose such information and data (the "Confidential Information") to any third party without Client's prior written consent.

("**Representatives**") who (i) have a need to know, for the purpose of this Work Order; and (ii) are under written obligations of confidentiality that protect Confidential Information from unauthorized use and disclosure. Confidential Information does not include (i) information that has been or is, prior to this Work Order, in the public record, or is placed in the public record by Client after the Work Order begins; (2) facts concerning the provision of services and transactions between the parties (which do not constitute work product) necessary to set forth in proceedings for non-payment of invoices; and (3) anonymous data, configurations, specifications, and other conditions that are identified as vulnerabilities, anomalies, gaps identified by CyberDnA.

Cyber DnA acknowledges that the unauthorized use or disclosure of Client's Confidential Information could cause irreparable harm to Client and that monetary damages would be inadequate compensation for any breach of this Work Order. Accordingly, CyberDnA agrees that Client shall be entitled to seek injunctive relief or other equitable relief in addition to any other remedy it may have at law or in equity against the threatened or actual breach of the confidentiality obligations herein or

3. Services CyberDnA will provide the following Services to Client:

**Phase 1- Red Teaming**

CyberDnA will be performing Red Team exercise to Client internal corporate network to understand the attack surface and the degree of exploitability and to offer recommendations that would help the client to prevent, detect and contain threats to its systems. The Scope of this exercise would involve perform internal security testing to understand the state of security and the incident handling capability of Client. The focus of this exercise will be to achieve the objectives in an effective manner using tactics that Client would be subjected to in a realistic scenario, as opposed to identifying as many vulnerabilities as possible within the organization's infrastructure and software. The same would be performed by achieving following objectives.

- Sending email with malicious attachment to assigned user id
- Compromising the machine assigned to CyberDnA Red Team using the inherent vulnerabilities
- Performing privilege escalation to obtain root privileges
- Creating a C2 channel from the compromised machine to communicate outside the Kotak network
- Scanning the network to understand topology and restrictions
- Lateral movement to other machines
- Pivoting and executing various attacks (Pass the hash, Kerberoasting, PowerShell, scripts)
- Mapping the critical servers in the network
- Attempting to compromise the critical servers and provide evidence
- Identifying gaps in network security measures, incident response and monitoring process such as detection time and reaction time
- Recommending measures to strengthen the existing security architecture

**Phase 2 – Priority Asset Penetration Testing**

- Penetration Testing for Client's key business applications and underlying infrastructure
- The scope includes assessment of 68 web application, 500 IPs for infrastructure.
- The external assessment for internet facing applications and infrastructure would carried out from CyberDnA's premises.
- Confirmatory assessment would be performed to confirm remediation fixes applied.
- Black Box methodology would be followed for 68 web applications and 500 IPs for infrastructure.
- Data exfiltration and proof of concepts of exploitation would be taken to understand the impact of the vulnerabilities identified.

**Engagement limitations**

This is an yearly assessment. The assessment was based on existing body of knowledge and not designed to detect all weaknesses in controls. Accordingly, changes in circumstances or control environment after our review could affect the findings outlined in this report.

The procedures we will be performing under this Agreement will not constitute an examination or a review in accordance with generally accepted auditing standards or attestation standards. CyberDnA will not audit or otherwise verify the information supplied to us in connection with any engagement under this Agreement, from whatever source, except as may be specified in this Agreement.

Our report will be addressed to the management of Client and will be intended for solely for internal use of Client. Neither the report nor its contents may be distributed, discussed or disclosed to any third party without the prior written consent of CyberDnA.

Our procedures under this engagement are not designed to and are not likely to reveal fraud or misrepresentation by the management of Client. Accordingly, we cannot accept responsibility for detecting fraud (whether by management or by external parties) or misrepresentation by the management of Client or any other person.

**Key Assumptions and Limitations**

- The scope, content and format for all key deliverables will be discussed and agreed in advance between client and CyberDnA prior to the commencement of work.
- All information required for the project will be made available within two (2) business days from our request to the Client.
- For achieving project efficiencies, CyberDnA may carry out multiple activities in parallel either onsite or offsite.
- Client will designate a Project Coordinator who will be the single point of contact for CyberDnA who will be responsible for liaising with CyberDnA on a daily basis.
- Emails will be considered as official form of written communication and any representations, approvals on email will be considered to be equivalent of written memos.
- CyberDnA Consultants will help the involved stake holders understand the Business risk and the Criticality of the Vulnerability.
- CyberDnA Consultants will not be a part of active remediation. Only remediation recommendations would be provided as a part of this activity.
- CyberDnA will retest the application tested after the remediation has been completed by the Client stake holders.
- CyberDnA will need to understand if there are any Cloud Infrastructure too. If yes, then the details of the agreement with the vendor with respect to performing penetration testing services.

- CyberDnA will not be responsible for implementation of the recommendations provided or addressing any threats/ vulnerabilities.
- The scope of work will be ongoing yearly exercise for CyberDnA

Furthermore, CyberDnA has requested Client to preserve the identified electronic devices as it may be required at some point to capture network traffic to review the contents leaving the gateway.

The Parties acknowledge that the procedures set out above shall serve as a guide and may be modified by mutual agreement during the course of the engagement.

## 4. Deliverables

For the purpose of this engagement, CyberDnA's Client is Vital Management, CyebrDnA will prepare a report based on the facts and findings of CyberDnA's work under this Work Order (the "Report"). The Report should not be relied upon by any other party. CyberDnA will not accept any responsibility or liability to a third party to whom the Report may be shown or in whose hands it may come. CyberDnA shall maintain its confidentiality obligations to Client with regards to all deliverables created for, and all communications with, Client under this Work Order pursuant to Section 2 of this Work Order.

In the event CyberDnA is requested or authorized by the Client (subject to written consent of CyberDnA in agreeing to such request/authority) or if CyberDnA is mandatorily required by applicable government regulation, or a subpoena or other legal process authorized by a competent governmental or judicial authority to produce any deliverable or its personnel as witnesses with respect to the work performed under this Work Order, Client shall, in addition to the fees under this Work Order, fully reimburse CyberDnA for its professional time and expenses on the rates applicable at that time, as well as the fees and expenses of legal counsel (if incurred by CyberDnA) in responding to that request. However, CyberDnA shall, if permitted under applicable law, promptly notify Client in writing that it has received a request made under authority of a governmental or judicial authority in order to provide Client with the opportunity, if available, to prevent or limit the disclosure of any such deliverable.

## 5. Timetable

CyberDnA will commence the Services on 1st September 2019 and estimates that it will submit its draft deliverables to Client for discussion by March 2020 for Phase 1 and September 2020 for Phase 2. This is an estimate in advance of starting work and CyberDnA will keep Client informed of its progress and of any proposed changes in this timetable.

Above timeline is dependent upon timely receipt of information by CyberDnA and subject to CyberDnA receiving full co-operation and assistance from Client's staff. In case of technical issues and unusual delays we will report the same to Client and discuss with Client the course of action to be taken. The above timeline may also suitably change depending upon scope modifications which may occur during the course of the engagement.

## 6. Fees and expenses

CyberDnA's fees may reflect factors including time spent, complexity, urgency, inherent risks, use of techniques, know-how and research together with the level of skills and expertise required of the personnel needed to perform and review the Services.

For Phase 1 the fee payable is USD 10000 per month on a retainer model for single annual cycle.

For Phase 2 the fee payable is USD 15000 per month on a retainer model for single annual cycle.

Client will pay any out of pocket expenses on actuals that CyberDnA reasonably incurs in connection with the Services.

The Professional fees exclude taxes as applicable and out of pocket expenses ("OPEs") necessary for the assignment such as travel, accommodation costs, conveyance, communication costs, etc., which would be billed at actual.

CyberDnA will raise our invoice on issuance of the Report, and non-disputable charges in the invoice are payable within 45 days from receipt.

## 7. Client responsibilities

CyberDnA's role is of an advisory nature only and excludes taking management decisions or acting in a management or employee capacity. Client is responsible for all management and employee functions and decisions relating to this engagement, including evaluating and accepting the adequacy of the scope of the Services in addressing Client's needs. Client is also responsible for the results achieved from using any Services or deliverables. Client will designate appropriate members of its management to oversee the Services. Additionally, it is Client's responsibility to provide the necessary resources to implement any changes Client wishes to make as a result of CyberDnA's findings

Additionally, CyberDnA's Services do not include the provision of legal advice, and CyberDnA makes no representations regarding questions of legal interpretation.

## 8. Law and jurisdiction

This Contract and any dispute arising from it, whether contractual or non-contractual, will be governed exclusively by Indian law and be subject to the exclusive jurisdiction of the Indian courts

*This Work Order is effective from May 6th, 2019.*

know-how and research together with the level of skills and expertise required of the personnel needed to perform and review the Services.

For Phase 1 the fee payable is USD 10000 per month on a retainer model for single annual cycle.

For Phase 2 the fee payable is USD 15000 per month on a retainer model for single annual cycle.

Client will pay any out of pocket expenses on actuals that CyberDnA reasonably incurs in connection with the Services.

The Professional fees exclude taxes as applicable and out of pocket expenses ("OPEs") necessary for the assignment such as travel, accommodation costs, conveyance, communication costs, etc., which would be billed at actual.

CyberDnA will raise our invoice on issuance of the Report, and non-disputable charges in the invoice are payable within 45 days from receipt.

## 7. Client responsibilities

CyberDnA's role is of an advisory nature only and excludes taking management decisions or acting in a management or employee capacity. Client is responsible for all management and employee functions and decisions relating to this engagement, including evaluating and accepting the adequacy of the scope of the Services in addressing Client's needs. Client is also responsible for the results achieved from using any Services or deliverables. Client will designate appropriate members of its management to oversee the Services. Additionally, it is Client's responsibility to provide the necessary resources to implement any changes Client wishes to make as a result of CyberDnA's findings

Additionally, CyberDnA's Services do not include the provision of legal advice, and CyberDnA makes no representations regarding questions of legal interpretation.

## 8. Law and jurisdiction

This Contract and any dispute arising from it, whether contractual or non-contractual, will be governed exclusively by Indian law and be subject to the exclusive jurisdiction of the Indian courts

*This Work Order is effective from May 6th, 2019.*

| | |
|---|---|
| Signed on behalf of Cyber Defence and Analytics<br>by: | Signed on behalf of Vital Management Services,Inc. |
| Name: Aditya Jain<br>Title: Proprietor<br>Date: May 5th, 2019 | Name:<br>Title:<br>Date: |